САЙФЕР

Построение долговременного архива электронных документов

ООО “Сайфер БИС”: Влад Ковтун
Александр Стокипный
Андрей Охрименко

САЙФЕР

Куда движемся? В облако!

Активное развитие облачных технологий формирует новые вызовы перед сервисами и приложениями реализующими криптографические операции.

В портфеле компании Сайфер имеется целый ряд решений ориентированных на развертывание в облачной инфраструктуре:

- Шифр-CaaS
  - BankID НБУ
  - MobileID (Vodafone, Lifecell)
- Агент Шифр-CaaS
- Шифр-Signer (Сервис подписи)
- Шифр-Crypto (Сервис шифрования)
- Персональный сервис подписи

Также активно ведется разработка целого ряда проектов, которые пополнят семейство облачных решений компании Сайфер. Об одном из них поговорим и сейчас!

Куда движемся? В IoT!

Непрерывное увеличение числа IoT устройств и проникновение этих устройств во все сферы человеческой деятельности потребовало обеспечить их защиту и данных на устройствах!

В портфеле компании появилось полноценное решение Шифр-IoT, которое позволяет реализовывать функции:

- Механизмы сопровождения процесса разработки
- Cryptography as a Service
- PKI & CA
- Комплект ПО для первичной инициализации устройства
- Механизм защищенного обновления устройства
- Механизм удаленной переинициализации устройства

Intro

Переход на обмен документами, которые существуют исключительно в электронном виде, особенно, если документы предназначены не только для внутреннего использования, но и могут быть использованы в разрешении возможных споров. Как правило, такие документы обладают квалифицированной электронной подписью (КЭП).
Сроки хранения таких документов измеряются десятилетиями, причем существует необходимость в проверке ЭП всеми подписантами, для установления:

- Целостности документа.
- Авторства.
- Неотказуемости.

Особенно актуальны вопросы продолжительности хранения электронных документов для государственного, банковского и страхового сектора.

Подходы

- **Стандартный**. Использование ЭП в формате CAdES X-Long, которая позволяет обеспечить долговременную проверку ЭП.
  - Решение о корректности ЭП принимается, когда она успешно проверяется, при получении/создании.
  - По истечению определенного периода времени невозможно проверить ЭП согласно действующим нормативным документам.
- **Расширенный (Blockchain**). В дополнение к Стандартному подходу, использование модифицированных механизмов сцепления блоков, на основе имитовставки.
  - Решение о корректности ЭП принимается, когда она успешно проверяется, при получении/создании.
  - Сама ЭП и результаты ее проверки, а также все используемые для проверки данные заносятся в БД и сцепляются с предыдущими записями с помощью имитовставки.
  - При проверке ЭП, непосредственно сама ЭП не проверяется, а лишь проверяется целостность всех сцепленных записей в БД.

САЙФЕР

Что есть на рынке Украины?

Отметим, что существующие на украинском рынке решения по доставке и обмену электронными документами с ЭП не обеспечивают их долговременное хранение:

- Исключительно проверка ЭП/КЭП
- Целостность средствами БД

САЙФЕР

Стандартный подход

Недостатки

- Ограниченный срок гарантированной проверки ЭП:
  - Срок действия сертификата ЦУО (ЦУО)
  - Срок действия сертификата ЦСК (ЦУО)
  - Срок действия сертификата OCSP (ЦСК)
  - Срок действия сертификата TSP (ЦУО)
- Возможность компрометации используемых ключей
- Возможность отказа от существующих стандартов ЭП, по причине их морального устаревания
- Необходимость расширения ЭП до формата CAdES X-Long
- Проверка ЭП из архива онлайн с ЦСК и ЦУО

Преимущества

- Простота использования
- Отсутствие БД
- Отсутствие необходимости в обеспечении дополнительных механизмов защиты
- Документы хранятся в отдельной системе

САЙФЕР

Расширенный подход

Недостатки

- Сложность решения
- Необходимость ведения БД с откреплённой ЭП сцепленными записями
- Необходимость периодически производить проверку целостности всей БД с сцепленными записями
- Необходимость расширения ЭП до формата CAdES X-Long
- Необходимость в обеспечении защиты ключа имитовставки для сцепления блоков

Преимущества

- Неограниченный срок гарантированной проверки ЭП, т.к. сама ЭП не проверяется, а лишь проверяется целостность сцепленных записей в БД с откреплённой ЭП
- Компрометации используемых ключей не влияет, на уже проверенные ЭП
- Отказ от существующих стандартов ЭП не влияет, на уже проверенные ЭП
- Документы хранятся в отдельной системе
- Проверка ЭП из архива в офлайн (без ЦСК и ЦУО)

САЙФЕР

Стандартный подход. Функции

- Проверка ЭП, перед занесением документа в архив*
  - Проверка ЭП
    - Отправка запросов в ЦУО (OCSP)
    - Отправка запросов в ЦСК (OCSP)
  - Расширение ЭП до CAdES X-Long (в случае необходимости)
- Проверка ЭП в формате CAdES X-Long и документа из архива*
  - Проверка ЭП
    - Отправка запросов в ЦУО (OCSP)
    - Отправка запросов в ЦСК (OCSP)

*- ЭП подпись хранится вместе с документами в архиве

САЙФЕР

Расширенный подход

Шифр-Arch

Система ведения долговременного архива электронных документов организации

САЙФЕР

Шифр-Arch. Характеристики

Система ведения долговременного архива позволяет:

- Работать сразу в нескольких ЦОД, в виде единого кластера
- Работать автономно в каждом ЦОД, если единый кластер “развалился”
- Восстановление единого кластера, после его “развала”, на основе кластеров одного из ЦОД
- Горизонтальное масштабирование, до 32-х серверов в кластере БД с документами
- Хранение документов: не ограничено по объему (проверяли на 192 ТБ)
- Размер документа: до 5 ТБ
- Клонирование узлов со связанными цепочками для повышения доверия/защиты от подделки
- Аутентификация посредством JWT (JSON Web Token)
- Защита каналов связи:
    - Работа внутри системы через TLS
    - Работа с API через TSL
    - Web-интерфейс через HTTPS/TLS

САЙФЕР

Шифр-Arch. Функции

- Проверка ЭП, перед занесением документа в архив*
  - Проверка ЭП
    - Отправка запросов в ЦУО (OCSP)
    - Отправка запросов в ЦСК (OCSP)
  - Расширение ЭП до CAdES X-Long (в случае необходимости)
  - Дополнительно можно добавить, к ЭП документа:
    - ЭП ответственного сотрудника (архиариуса)
    - Печать организации
  - Добавление откреплённой ЭП, хеш-образа документа и результатов проверки ЭП в БД со сцепленными записями
- Полнотекстовый поиск документа по реквизитам и подписантам (текст документа не индексируется)

*- ЭП подпись хранится в БД архива ЭП со сцепленными записями, без документов

САЙФЕР

Шифр-Arch. Функции и Роли

- Проверка ЭП, перед занесением документа в архив*
- Проверка целостности документа из архива
  - Сопоставление хеш-образа документа и записи из БД со сцепленными записями
  - Принятие решение по результатам консолидированной проверки из нескольких узлов
- Проверка целостности БД со сцепленными записями (несколько таких БД)
  - Проверка целостности БД со сцепленными записями, посредством ее воспроизведения
  - Принятие решение по результатам консолидированной проверки из нескольких узлов
  - По расписанию

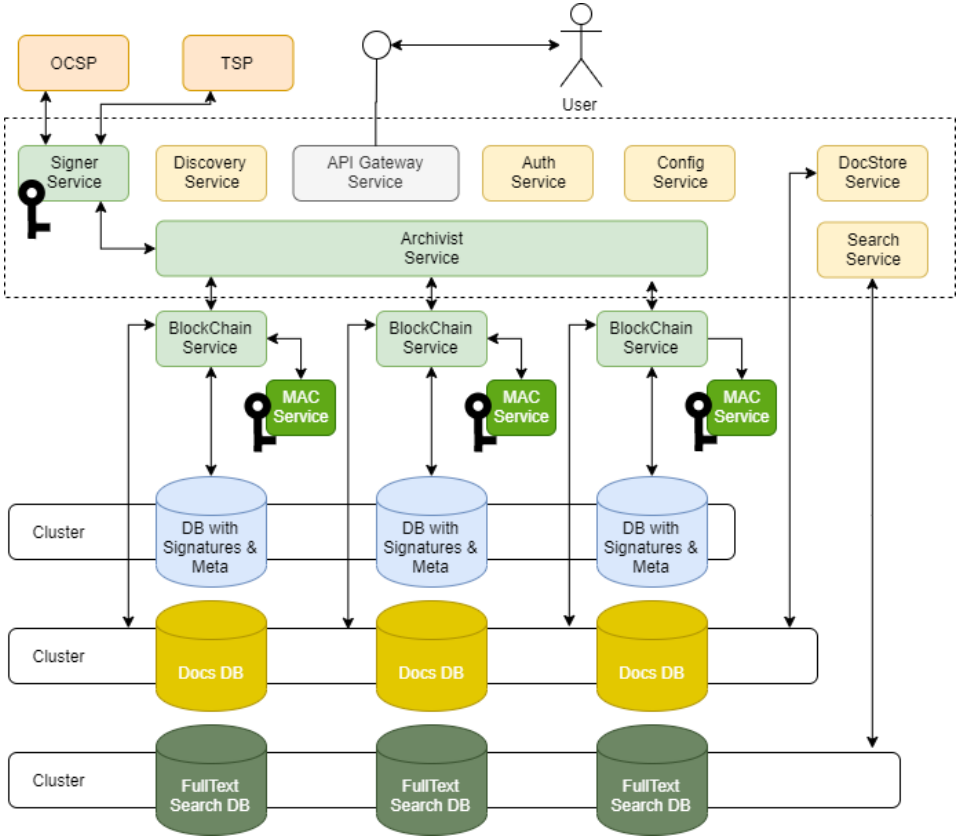
Ролевая модель:

- Администратор
- Оператор

*- ЭП подпись хранится в БД архива ЭП со сцепленными записями, без документов

САЙФЕР

Шифр-Arch. Архитектура



- Микросервисы:
  - Сервис шлюз API
  - Сервис аутентификации
  - Сервис поиска
  - Сервис хранения электронных документов
  - Сервис архивирования
  - Сервис сцепления блоков
  - Сервис подписи
  - Сервис кодов аутентификации
  - Сервис обнаружения
  - Сервис хранения конфигурации
  - Сервис логирования
  - Сервис мониторинга

Шифр-Arch. Архитектура

Система архивирования строится на основе микросервисной архитектуры:

- БД:
  - Block/Object БД Cluster (S3-like Storage)
  - Object DB Cluster
  - Full Text Search DB Cluster
- Сервис хранения конфигурации
- Web-клиент, по работе с API (пользователь)
- Web-клиент, по работе с API (администратор)
- Система логирования
  - Kibana
  - Logstash
  - Elasticsearch
- Система мониторинга
  - Grafana
  - Prometheus

Используемые технологии:

- Контейнеры: Docker
- Оркестрирование: Docker Swarm / Kubernetes

САЙФЕР

Шифр-Arch. Развертывание

Система строится на основе:

- Open Source решений (enterprise, production ready)
  - Возможна расширенная поддержка со стороны разработчиков
- Криптографических библиотек компании “Сайфер”, имеющих позитивные экспертные заключения Госспецсвязи
  - Возможна расширенная поддержка со стороны компании “Сайфер”

Развертывание допустимо:

- Public Cloud (DeNovo, GigaCloud, Парковый, uCloud, GCP, AWS, Azure)
- Private Cloud
- Bare Metal
- Смешанная

Шифр-Arch. Криптография

Используемые криптографические алгоритмы:

- ЭП/КЕП:
  - ДСТУ 4145+ГОСТ 34.311-95 (по умолчанию)
  - ДСТУ 4145+ДСТУ 7624:2014*
  - ECDSA+SHA-256*
  - RSA+SHA-256*
- Hash:
  - ГОСТ 34.311-95
  - ДСТУ 7564:2014
  - SHA-2 семейство
- MAC (используется для сцепления блоков):
  - ДСТУ ГОСТ 28147:2009
  - ДСТУ 7624:2014 (по умолчанию)
  - AES (AES-NI)

*- пока не востребовано, возможно подключить в дальнейшем

Шифр-Arch. Криптография

Используемые хранилища ключей:

- ЭП/КЕП:
  - PFX/PKCS#12/Key-6.dat (по умолчанию)
  - PKCS#11-пассивный режим
  - PKCS#11-активный режим (Network HSM)
- MAC:
  - PKCS#12 (по умолчанию)
  - PKCS#11-активный режим (Network HSM)

САЙФЕР

Шифр-Arch. Внедрения

Существующие внедрения показали:

- Высокую производительность при работе с документами
- Снижение стоимости хранения документа, за счет снижения стоимости владения системой в целом (отказ от стандартных решений, как Oracle DB, Microsoft SQL Server)
- Надежность работы
- Современные технологии
- Легкость масштабирования

Наибольший интерес долговременные архивы электронных документов представляют:

- Государственный сектор
- Банковский сектор
- Страховой сектор

Отдельно следует выделить АЦСК/КПЭДУ, для реализации соответствующей услуги

САЙФЕР

Спасибо за внимание!

Александр Стокипный: as@cipher.com.ua

Андрей Охрименко: ao@cipher.com.ua

Влад Ковтун: vk@cipher.com.ua